

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051
<http://oversight.house.gov>

Opening Statement Rep. Elijah E. Cummings, Ranking Member

Hearing on "Security Clearance Reform: The Performance Accountability Council's Path Forward"

February 25, 2016

Mr. Chairman, I appreciate you holding today's hearing to discuss the Administration's plan to make significant changes to the federal government's background check operations and the way it secures the personal and sensitive information gathered in those checks. This is precisely the type of hearing our Committee should be having, looking across agencies at new proposals to improve the effectiveness and efficiency of government. So thank you again.

In 2013, a disturbed Navy contractor with a security clearance shot and killed 12 people and injured 4 others here in Washington, D.C. Our Committee conducted an investigation of that terrible shooting, and we found that a contractor, USIS, conducted the shooter's background check. We found that USIS failed to include information on his previous arrest for shooting out the tires of his neighbor's car. As a result, he was given a "secret" level security clearance.

We also found that USIS committed fraud against the American taxpayers on a much wider scale by submitting incomplete background investigations. USIS ultimately agreed to the demands of the Justice Department to forego \$30 million as a result of its actions, and it no longer conducts background checks on behalf of the federal government. I ask unanimous consent that the report I issued on this topic be entered into the hearing record.

Then, last year, cyber attackers successfully breached OPM's data systems. Again, our Committee investigated, and again we found the weak link in the chain was a contractor. We heard testimony explaining that these cyber attackers were able to gain access to federal systems by using KeyPoint's privileged access to OPM's networks. As a result, the personal information of millions of federal employees with security clearances was compromised.

These cyber attacks on OPM were not isolated incidents. Other federal contractors, including Anthem and Premera, were also attacked. Experts believe these were all part of a sophisticated, coordinated cyber-espionage campaign. They all occurred at about the same time, they all targeted sensitive information about federal employees, and they all were carried out using similar malware.

The proposal we are discussing today is a significant and substantive response to these events, and it is more than just the new National Background Investigations Bureau. The Administration's proposal leverages the expertise of key parts of the government, like the Department of Defense, to provide critical IT and cyber security capabilities. I believe this is a serious effort to combat sophisticated cyber attackers who are targeting our government, and it deserves serious consideration by Congress.

Today, I want to hear more about how this proposal will address the significant problems we have had with contractors. The government's reliance on contractors helps supplement the workforce and increase our capabilities, but as we have seen, it also carries major risks. I want to know how the Administration's proposal will increase oversight and accountability over contractors charged with safeguarding some of our nation's most sensitive information.

Let me address two final points. First, earlier this week, Donna Seymour, OPM's Chief Information Officer, retired after more than 35 years of service to her country. Unfortunately, some have inaccurately blamed Ms. Seymour for pre-existing vulnerabilities she inherited.

Now, I was one of the most vocal critics of the CIO's office at our last hearing because the Inspector General raised concerns about obtaining access to information from that office. And I continue to believe those concerns were valid. However, our investigation has now found that the cyber attacks against OPM were already underway when Ms. Seymour took office in December 2013. In addition, experts in and out of the agency informed us that she helped uncover the attack, she led an aggressive response, and she elevated cyber security to a top priority when previously it had languished.

So I believe these recent political attacks against Ms. Seymour are both unfair and inaccurate. They also set a terrible precedent that will discourage qualified experts from taking on the challenges our nation faces in the future.

Finally, on that same note, as we sit here today, certain Republicans in the Senate are holding up the nomination of Beth Cobert as OPM Director for political reasons that have nothing to do with her qualifications for the position.

Just as Republicans are threatening to block anyone the President nominates to the Supreme Court for political reasons, they are stalling Ms. Colbert's nomination despite the fact that she has been widely praised for turning things around at the agency. The Inspector General has praised her efforts, and even some of her critics in Congress have praised her leadership. There is absolutely no reason to continue playing politics, and I hope every member of our Committee will join me today in asking the Senate to confirm President Obama's nomination for this position as soon as possible.

Thank you again, Mr. Chairman, for calling this important hearing, and I look forward to the testimony of our witnesses here today.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.